W dniu 13.05.2019 r. dodano informację dot. rozstrzygnięcia procedury zapytania ofertowego na dostawę i instalację w siedzibie zamawiającego zintegrowanego systemu bezpieczeństwa w ramach zadania 8 „Doposażenie sieci" w związku z realizowanym przez Gminę Ostróda projektem pn.: „Informatyzacja urzędu i wdrożenie nowoczesnych e-usług w Gminie Ostróda".

Ostróda, dnia 13.05.2019r.

INF.271.2.2019

Informacji o rozstrzygnięciu procedury zapytania ofertowego, na dostawę i instalację w siedzibie zamawiającego zintegrowanego systemu bezpieczeństwa w ramach zadania 8 „Doposażenie sieci" w związku z realizowanym przez Gminę Ostróda projektem pn.: „Informatyzacja urzędu i wdrożenie nowoczesnych e-usług w Gminie Ostróda".

W związku z zakończeniem procedury zapytania ofertowego w dniu 10.05.2019r., zgodnie z zasadą rozeznania rynku w odpowiedzi na zapytanie ofertowe opublikowane 29.04.2019 r. na podmiotowej stronie internetowej Biuletynu Informacji Publicznej Urzędu Gminy Ostróda www.bip.gminaostroda.pl, dotyczące dostawy i instalacji w siedzibie zamawiającego zintegrowanego systemu bezpieczeństwa w ramach zadania 8 „Doposażenie sieci":

Złożono trzy oferty:
1. NBIT, Marta Wołoszyn, 44-100 Gliwice, ul. Chodkiewicza 31 - **46 924,50 zł.**
2. 4NetiC,Marzena Zera, 11-500 Giżycko, Wilkasy ul. Lipowa 29 - **37 490,40 zł.**
3. Ikaria, Łukasz Gil, ul. Omłotowa 12/14, 94-251 Łódź - **50 928,15 zł.**

Wszyscy trzej oferenci spełnili wymogi specyfikacyjne, **a najtańszą ofertą** okazała się oferta **nr 2 firmy 4NetiC**, Marzena Zera, 11-500 Giżycko, Wilkasy ul. Lipowa 29 w cenie brutto **37 490,40 zł.**

W ramach oferty Dostawca zobowiązał się zgodnie z wymogami specyfikacyjnymi dostarczyć, zainstalować i wdrożyć w siedzibie Zamawiającego następujące elementy zintegrowanego systemu bezpieczeństwa w postaci:

L.p.	Nazwa potoczna	Nazwa produktu
1.	Router	FortiGate-100EF Hardware
2.	5 lat licencji na oprogramowanie	BDL 8x5 FortiCare and FortiGuard Unified (UTM) Protection - 5 lat
3.	Moduł WiFi	FortiAP-423E
4.	5 lat licencji na oprogramowanie	FortiAP-423E 8x5 Enhanced FortiCare 5 lat
5.	Zasilacz	AC Power Adaptor for FAP-U423EV (zasilacz)

Ostróda, dnia 29 kwietnia 2019 roku

Nr postępowania: INF.271.2.2019

Zapytanie ofertowe na:

Dostawę i instalację w siedzibie zamawiającego zintegrowanego systemu bezpieczeństwa w ramach zadania 8 „Doposażenie sieci" w związku z realizowanym przez Gminę Ostróda projektem pn.: „Informatyzacja urzędu i wdrożenie nowoczesnych e-usług w Gminie Ostróda".

Przedmiot zamówienia jest współfinansowany z Europejskiego Funduszu Rozwoju Regionalnego, w ramach Regionalnego Programu Operacyjnego Województwa Warmińsko-Mazurskiego na lata 2014-2020, w ramach Osi Priorytetowej 3 „Cyfrowy Region", Działania 3.1 „Cyfrowa dostępność informacji sektora publicznego oraz wysoka jakość e-usług publicznych".

I. Zamawiający:

1. Zamawiający: Gmina Ostróda.

2. Adres Zamawiającego: Urząd Gminy Ostróda, ul. Jana III Sobieskiego 1, 14-100 Ostróda.

3. Adres e-mail: **sekretariat@gminaostroda.pl**.

4. Strona internetowa Zamawiającego: **www.gminaostroda.pl**.

5. tel./fax. 89 676 07 80/ 89 676 07 90.

II. Tryb udzielenia zamówienia:

Postępowanie prowadzone o udzielenie zamówienia publicznego w trybie zapytania ofertowego, zgodnie z zasadą rozeznania rynku w rozumieniu Wytycznych w zakresie kwalifikowalności wydatków w ramach Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego oraz Funduszu Spójności na lata 2014 - 2020 z dnia 19 lipca 2017r.

III. Opis przedmiotu zamówienia:

1. Zamówienie obejmuje dostawę i instalację w siedzibie zamawiającego zintegrowanego systemu bezpieczeństwa dostarczającego funkcjonalności: firewall, VPN, antywirus, IPS (ochrona przed atakami), filtrowanie treści WWW, ochrona przed spamem, DLP (ochrona przed wyciekiem informacji poufnej), kontrola aplikacji, optymalizacja pasma, kontroler sieci bezprzewodowych, uwierzytelnianie wraz z subskrypcją dla oprogramowania zarządczego w ramach Gwarancji 5 lat.

2. Szczegółowy opis potrzeb Zamawiającego, zawierający rodzaj i ilość sprzętu oraz ich specyfikacja techniczna została zawarta w Szczegółowej Specyfikacji Zamówienia stanowiącej **załącznik nr 2** do zapytania ofertowego. Wymieniony w Szczegółowej Specyfikacji Zamówienia sprzęt powinien być fabrycznie nowy, nieużywany, posiadać karty gwarancyjne i instrukcję obsługi w języku polskim oraz musi posiadać dokumenty wymagane obowiązującymi przepisami prawa potwierdzające oznakowanie CE (deklaracja zgodności lub certyfikat CE). Zamawiający informuje, że brak podania przez Wykonawcę producenta i modelu wyspecyfikowanego sprzętu, spowoduje odrzucenie oferty jako niezgodnej z treścią formularza zapytania ofertowego, z uwagi na fakt braku możliwości sprawdzenia oferowanego sprzętu pod kątem minimalnych wymagań zamawiającego, opisanych w załączniku nr 2.

3. Wykonawca uprawniony jest do przedstawienia w ofercie rozwiązań technicznych równoważnych, o nie gorszych parametrach wskazanych w załączniku 2 szczegółowej specyfikacji. Wykonawca powinien określić ich parametry, celem wykazania, że spełniają warunki określone w opisie przedmiotu zamówienia. Rozwiązania równoważne, zgodnie ze swoją definicją, muszą posiadać parametry oraz spełniać standardy nie gorsze niż szczegółowy opis przedmiotowego zamówienia zawarty w załączniku 2.

4. W miejscu gdzie Zamawiający dokonuje opisu przedmiotu zamówienia przez odniesienie do norm, europejskich ocen technicznych, aprobat, specyfikacji technicznych i systemów referencji technicznych, Zamawiający dopuszcza rozwiązania równoważne opisywanym, a odniesieniu takiemu towarzyszą wyrazy 'lub równoważne'.

5. Koszt dostawy należy uwzględnić w cenach jednostkowych dostarczanych produktów i nie powinien stanowić odrębnej pozycji na fakturze/rachunku.

6. Kod CPV: 32424000-1, Infrastruktura sieciowa.

IV. Termin wykonania zamówienia

Zamawiający wymaga aby zamówienie było zrealizowane maksymalnie do 7 dni roboczych od dnia zawarcia umowy. Termin wykonania zamówienia będzie liczony od dnia następnego po dniu podpisania umowy.

V. Przygotowanie oraz sposób złożenia oferty:

1. Wykonawca zobowiązany jest przygotować ofertę w sposób określony w niniejszym zapytaniu ofertowym.

2. Wykonawca może złożyć tylko jedną ofertę.

3. Ofertę należy sporządzić w języku polskim, na komputerze lub inną trwałą i czytelną techniką.

4. Oferta powinna być podpisana przez Wykonawcę lub przez osobę uprawnioną do reprezentowania Wykonawcy, ewentualne poprawki powinny być naniesione w sposób czytelny i parafowane przez osobę uprawnioną do złożenia oferty.

5. Na ofertę składa się wypełniony formularz ofertowy z podaniem ceny na całość zamówienia zgodnie z **załącznikiem nr 1** do zapytania ofertowego.

VI. Miejsce i termin składania ofert.

1. Ofertę należy przesłać pocztą, złożyć osobiście w siedzibie Zamawiającego, lub przesłać drogą elektroniczną na adres informatyk@gminaostroda.pl (podpisany skan dokumentów) nie później niż do dnia 10 maja 2019 roku. Decyduje data wpływu do Zamawiającego. Oferty złożone po tym terminie nie będą podlegały rozpatrzeniu.

2. Wykonawca winien zamieścić informacje o Ofercie z zapisem: „Informatyzacja urzędu i wdrożenie nowoczesnych eUsług w Gminie Ostróda” - „Doposażenie Sieci” oraz podać swoją nazwę, adres i dane kontaktowe.

3. Oferty, które wpłyną na inny adres mailowy Zamawiającego nie będą podlegały rozpatrzeniu.

4. Wykonawca może wprowadzić zmiany w ofercie lub ją wycofać, pod warunkiem, że uczyni to przed upływem terminu na składanie ofert. Zmiana, jak i wycofanie oferty wymaga zachowania formy pisemnej.

VII. Sposób obliczenia ceny:

1. Zaproponowana i ustalona w ofercie cena powinna być obliczona jako całkowita

cena brutto (z podatkiem VAT).

2. Cena musi zawierać wszelkie koszty niezbędne do zrealizowania zamówienia w tym m.in. koszty transportu, montażu (jeśli wymagane), serwisu w okresie gwarancji itp.

3. Wykonawca musi uwzględnić wszystkie podatki, cła i inne koszty, które będą opłacane przez Wykonawcę w ramach umowy, powinny być doliczone do stawek, cen i ceny ostatecznej ustalonej przez wykonawcę w ofercie.

4. Należy przewidzieć cały przebieg dostaw, a wszystkie utrudnienia wynikające z warunków realizacji Wykonawca winien uwzględnić w zaproponowanej cenie.

5. Zamawiający nie przewiduje waloryzacji wynagrodzenia (cen jednostkowych) przez okres realizacji zamówienia.

VIII. Kryteria oceny ofert

Cena 100%

IX. Osoby upoważnione do kontaktu z wykonawcami:

Osobą upoważnioną przez Zamawiającego do kontaktu z Wykonawcą jest Artur Jabłonka, tel. 89 676 07 27, e-mail: informatyk@gminaostroda.pl.

X. Termin związania ofertą:

1. Wykonawcy będą związani ofertą przez okres 7 dni od terminu składania ofert.

2. Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składnia ofert.

XI. Warunki płatności:

1. Rozliczenia między Zamawiającym a Wykonawcą prowadzone będą wyłącznie w PLN.

2. Wynagrodzenie będzie płatne po wykonaniu zamówienia przelewem na rachunek bankowy wskazany przez Wykonawcę w terminie do 14 dni od daty doręczenia prawidłowo wystawionej faktury do siedziby Zamawiającego.

3. Szczegółowe zasady rozliczenia finansowego pomiędzy Zamawiającym a Wykonawcą określi umowa na wykonanie przedmiotu zamówienia.

XII. Załączniki do zapytania ofertowego:

1. Formularz ofertowy załącznik nr 1 do zapytania ofertowego.

2. Specyfikacja techniczna załącznik nr 2 do zapytania ofertowego.

załącznik Nr 1

Nr postępowania: INF.271.2.2019

Formularz ofertowy do zapytania ofertowego na:

Dostawę i instalację w siedzibie zamawiającego zintegrowanego systemu bezpieczeństwa w ramach zadania 8 „Doposażenie sieci" w związku z realizowanym przez Gminę Ostróda projektem pn.: „Informatyzacja urzędu i wdrożenie nowoczesnych e-usług w Gminie Ostróda".

Dane Wykonawcy/Wykonawców wspólnie ubiegających się o udzielenie zamówienia

……

Nazwa (firma) / Imię i Nazwisko

……

Siedziba / miejsce zamieszkania i adres Wykonawcy

NIP……

REGON……

Dane kontaktowe:

Telefon/faks……

adres e-mail……

Oferujemy realizację przedmiotu zamówienia za cenę:

W tym miejscu Wykonawca przedstawi tabelaryczny wykaz poszczególnych elementów składających się na zintegrowany system bezpieczeństwa (nazwa produktu, ilość, cena jednostkowa netto, stawka VAT, wartość netto, wartość brutto, Razem netto, Razem brutto).

Oświadczenia i zobowiązania:

1. Oświadczamy, że zapoznaliśmy się z Zapytaniem ofertowym i nie wnosimy do niego zastrzeżeń oraz uzyskaliśmy konieczne informacje do przygotowania oferty.

2. Oświadczamy, że oferowany przez nas przedmiot zamówienia w pełni odpowiada wszystkim wymaganiom Zamawiającego określonym w Specyfikacji technicznej przedmiotu zamówienia (załącznik nr 2).

3. Oświadczamy, że uważamy się za związanych niniejszą ofertą na okres 7 dni.

4. Oświadczamy, że akceptujemy wskazany w Zapytaniu ofertowym termin i sposób płatności.

5. Oświadczamy, że oferowana przez nas całkowita cena brutto obejmuje wszystkie zobowiązania oraz wszystkie koszty związane z wykonaniem przedmiotu zamówienia oraz warunkami stawianymi przez Zamawiającego.

.....

Miejscowość, data

.....

Pieczęć i podpis osoby upoważnionej

Załącznik Nr 2

Nr postępowania: INF.271.2.2019

Specyfikacja techniczna do zapytania ofertowego na:

Dostawę i instalację w siedzibie zamawiającego zintegrowanego systemu bezpieczeństwa w ramach zadania 8 „Doposażenie sieci" w związku z realizowanym przez Gminę Ostróda projektem pn.: „Informatyzacja urzędu i wdrożenie nowoczesnych e-usług w Gminie Ostróda".

Wymagania Ogólne

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość

budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS. Powinna istnieć możliwość dedykowania co najmniej 8 administratorów do poszczególnych instancji systemu.

System musi wspierać IPv4 oraz IPv6 w zakresie:

• Firewall.

• Ochrony w warstwie aplikacji.

• Protokołów routingu dynamicznego.

Redundancja, monitoring i wykrywanie awarii

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.

2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.

3. Monitoring stanu realizowanych połączeń VPN.

4. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.

Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall musi dysponować minimum:

• 8 portami Gigabit Ethernet RJ-45.

• 8 gniazdami SFP 1 Gbps.

2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.

3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.

Parametry wydajnościowe:

1. W zakresie Firewall'a obsługa nie mniej niż 2 mln jednoczesnych połączeń oraz 30.000 nowych połączeń na sekundę.

2. Przepustowość Stateful Firewall: nie mniej niż 7.4 Gbps dla pakietów 512 B.

3. Przepustowość Stateful Firewall: nie mniej niż 4.4 Gbps dla pakietów 64 B.

4. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1 Gbps.

5. Wydajność szyfrowania VPN IPSec dla pakietów 512 B, przy zastosowaniu algorytmu o mocy nie mniejszej niż AES256 – SHA256: nie mniej niż 4 Gbps.

6. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu HTTP - minimum 1.9 Gbps.

7. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 250 Mbps.

8. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL (TLS v1.2 z algorytmem nie słabszym niż AES128-SHA256) dla ruchu http – minimum 190 Mbps.

Funkcje Systemu Bezpieczeństwa:

W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.

2. Kontrola Aplikacji.

3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.

4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.

5. Ochrona przed atakami - Intrusion Prevention System.

6. Kontrola stron WWW.

7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3, IMAP.

8. Zarządzanie pasmem (QoS, Traffic shaping).

9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).

10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.

11. Analiza ruchu szyfrowanego protokołem SSL.

12. Analiza ruchu szyfrowanego protokołem SSH.

Polityki, Firewall

System Firewall musi umożliwiać tworzenie list kontroli dostępu realizowanych bezstanowo przed funkcją FW.

1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.

2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:

• Translację jeden do jeden oraz jeden do wielu.

• Dedykowany ALG (Application Level Gateway) dla protokołu SIP.

3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.

Połączenia VPN

1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:

• Wsparcie dla IKE v1 oraz v2.

• Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).

• Obsługa protokołu Diffie-Hellman grup 19 i 20.

• Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.

• Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.

• Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.

• Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.

• Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.

• Mechanizm „Split tunneling” dla połączeń Client-to-Site.

2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:

• Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.

• Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta.

Routing i obsługa łączy WAN

1. W zakresie routingu rozwiązanie powinno zapewniać obsługę:

• Routingu statycznego.

• Policy Based Routingu.

· Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.

2. System musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN.

Zarządzanie pasmem

1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.

2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.

3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

Kontrola Antywirusowa

1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).

2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.

3. Moduł kontroli antywirusowej musi mieć możliwość współpracy z dedykowaną, komercyjną platformą (sprzętową lub wirtualną) lub usługą w chmurze typu Sandbox w celu rozpoznawania nieznanych dotąd zagrożeń.

Ochrona przed atakami

1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.

2. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.

3. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.

4. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.

5. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.

6. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

Kontrola aplikacji

1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.

2. Baza Kontroli Aplikacji powinna zawierać minimum 2100 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.

3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.

4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.

5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

Kontrola WWW

1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.

2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania),

phishing, spam, Dynamic DNS, proxy avoidance.

3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.

4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.

5. System musi umożliwiać zdefiniowanie czasu, który użytkownicy sieci mogą spędzać na stronach o określonej kategorii. Musi istnieć również możliwość określenia maksymalnej ilości danych, które użytkownik może pobrać ze stron o określonej kategorii.

6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.

Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:

• Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.

• Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.

• Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.

2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.

3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.

Zarządzanie

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.

2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.

3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.

4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły

SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.

5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.

6. System musi mieć wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.

Logowanie

1. System musi mieć możliwość logowania do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.

2. W ramach logowania system musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.

3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.

4. Musi istnieć możliwość logowania do serwera SYSLOG.

Certyfikaty

Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikaty:

• ICSA lub EAL4 dla funkcji Firewall.

• ICSA lub NSS Labs dla funkcji IPS.

• ICSA dla funkcji IPSec VPN.

• ICSA dla funkcji SSL VPN.

Serwisy i licencje

W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:

a) Kontrola Aplikacji, IPS, Antywirus, Antyspam, Web Filtering na okres 5 lat.

b) Logowanie do usługi realizowanej w chmurze na okres 5 lat.

Gwarancja oraz wsparcie

1. Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 5 lat, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 8x5.

Opisy do wymagań ogólnych

1. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.

2. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

Moduł WiFi tzw. Access Point

Urządzenie musi być tzw. cienkim punktem dostępowym zarządzanym z poziomu kontrolera sieci bezprzewodowej.

Obudowa urządzenia musi być wykonana z tworzywa sztucznego i umożliwiać montaż na suficie wewnątrz budynku.

Musi być wyposażone w dwa niezależne moduły radiowe pracujące w pasmach i obsługiwać następujące standardy:

1. 2.4 GHz b/g/n

2. 5 GHz a/n/ac

Urządzenie musi pozwalać na jednoczesne rozgłaszanie co najmniej 14 SSID

Liczba interfejsów Ethernet – 2 w standardzie 10/100/1000 Base-TX

Urządzenie powinno być zasilane poprzez interfejs ETH w standardzie 802.3at lub zewnętrzny zasilacz

Interfejs radiowy urządzenia powinien wspierać następujące funkcje:

1. MIMO – 4x4

2. Maksymalna przepustowość interfejsu dla poszczególnych pasm:

a) 2.4GHz – 600 Mbps

b) 5 GHz – 1733 Mbps

3. Wymagana moc nadawania min. 23 dBm

4. Wsparcie dla 802.11n 20/40Mhz HT

5. Wsparcie dla kanału 80 MHz dla 802.11ac

6. Złącza antenowe – RP-SMA. Wymagane dostarczenie w zestawie 8 anten zewnętrznych ze złączem RP-SMA o zysku min. 3dBi dla anten z pasma 2.4GHz, 3dBi dla anten z pasma 5GHz

7. Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 5 lat, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 8x5.

Data przekazania do publikacji: **29.04.2019**
Osoba przekazująca: **Artur Jabłonka**

Sporządził/a: **Artur Jabłonka**
Umieścił/a: **Artur Jabłonka**

data publikacji: 29.04.2019, ostatnia aktualizacja: 13.05.2019, odsłon: 692